AMENDMENT TO RULES COMMITTEE PRINT 117–54

OFFERED BY MR. MALINOWSKI OF NEW JERSEY

At the end of title LII, insert the following:

SEC. 52___. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY; CISA COMMERCIAL SATELLITE SYSTEM CYBERSECURITY CLEARINGHOUSE.

(a) STUDY.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

(2) REPORT.—Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall report to Congress on the study conducted under paragraph (1), which shall include information on—

(A) the effectiveness of efforts of the Federal Government in improving the cybersecurity of commercial satellite systems;

(B) the resources made available to the public, as of the date of the enactment of this Act, by Federal agencies to address cybersecurity risks and cybersecurity threats to commercial satellite systems;

(C) the extent to which commercial satellite systems are reliant on or are relied on by critical infrastructure and an analysis of how commercial satellite systems, and the cybersecurity threats to such systems, are integrated into Federal and non-Federal critical infrastructure risk analyses and protection plans;

(D) the extent to which Federal agencies are reliant on commercial satellite systems and how Federal agencies mitigate cybersecurity risks associated with those systems; and

(E) the extent to which Federal agencies coordinate or duplicate authorities and take other actions focused on the cybersecurity of commercial satellite systems.

(3) CONSULTATION.—In carrying out paragraphs (1) and (2), the Comptroller General of the United States shall coordinate with appropriate Federal agencies, including—

(A) the Department of Homeland Security;

(B) the Department of Commerce;

(C) the Department of Defense;

(D) the Department of Transportation;

(E) the Federal Communications Commission;

(F) the National Aeronautics and Space Administration; and

(G) the National Executive Committee for Space-Based Positioning, Navigation, and Timing.

(4) BRIEFING.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall provide a briefing to Congress relating to carrying out paragraphs (1) and (2).

(5) CLASSIFICATION.—The report under paragraph (2) shall be unclassified but may include a classified annex.

(b) CISA COMMERCIAL SATELLITE SYSTEM CYBERSECURITY CLEARINGHOUSE.—

(1) ESTABLISHMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director shall establish a commercial satellite system cybersecurity clearinghouse.

(B) REQUIREMENTS.—The clearinghouse shall—

(i) be publicly available online;

(ii) contain current, relevant, and publicly available commercial satellite system cybersecurity resources, including the recommendations consolidated under paragraph (2), and any other appropriate materials for reference by entities that develop commercial satellite systems; and

(iii) include materials specifically aimed at assisting small business concerns with the secure development, operation, and maintenance of commercial satellite systems.

(C) EXISTING PLATFORM OR WEBSITE.—The Director may establish the clearinghouse on an online platform or a website that is in existence as of the date of the enactment of this Act.

(2) CONSOLIDATION OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY RECOMMENDATIONS.—

(A) IN GENERAL.—The Director shall consolidate voluntary cybersecurity recommenda-

tions designed to assist in the development, maintenance, and operation of commercial satellite systems.

(B) REQUIREMENTS.—The recommendations consolidated under subparagraph (A) shall include, to the greatest extent practicable, materials addressing the following:

(i) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

(ii) Planning for retention or recovery of positive control of commercial satellite systems in the event of a cybersecurity incident.

(iii) Protection against unauthorized access to vital commercial satellite system functions.

(iv) Physical protection measures designed to reduce the vulnerabilities of a commercial satellite system's command, control, or telemetry receiver systems.

(v) Protection against jamming or spoofing.

(vi) Security against threats throughout a commercial satellite system's mission lifetime.

(vii) Management of supply chain risks that affect the cybersecurity of commercial satellite systems.

(viii) As appropriate, and as applicable pursuant to the requirement under paragraph (1)(b)(ii) (relating to the clearinghouse containing current, relevant, and publicly available commercial satellite system cybersecurity resources), the findings and recommendations from the study conducted by the Comptroller General of the United States under subsection (a)(1).

(ix) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems.

(3) IMPLEMENTATION.—In implementing this subsection, the Director shall—

(A) to the extent practicable, carry out such implementation as a public-private partnership;

(B) coordinate with the heads of appropriate Federal agencies with expertise and experience in satellite operations, including the entities described in subsection (a)(3); and

(C) consult with non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

(c) DEFINITIONS.—In this section:

(1) The term ''clearinghouse'' means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under subsection (b)(1).

(2) The term ''commercial satellite system'' means an earth satellite owned and operated by a non-Federal entity.

(3) The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(4) The term ''cybersecurity risk'' has the meaning given such term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(5) The term ''cybersecurity threat'' has the meaning given such term in section 102 of the Cy-

bersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(6) The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(7) The term ''small business concern'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).